The Reputation of Networks – LACNIC Region

Manish Karir, Kyle Creyts

(Merit Network Inc)

Arturo Servin

(LACNIC)

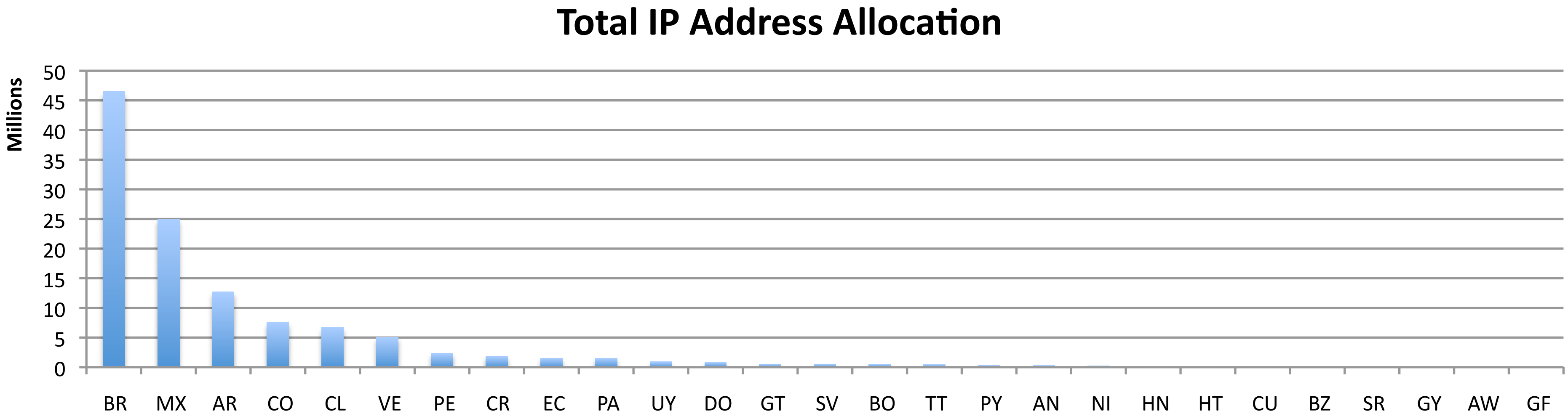
Outline

- Goal
- Background: IPv4 address allocation distribution in LACNIC, commonly used blocklists
- Analysis
  - foreach(country, asn, bgp prefix)
    - SPAM Lists Distribution
    - Malware/Phishing Lists Distribution
    - Active Malicious Activity Lists
    - Highlight points of interest in data
- Network Reputation Discussion

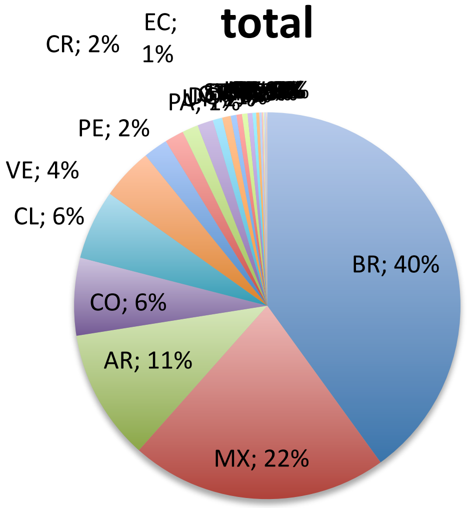
Common Reputation Block Lists (RBLs)

- RBLs are mostly lists of IP addresses of domains that have been observed to participate in suspicious behavior
- RBLs can be clustered by type of activity on which it is based:
  - SPAM Lists: SPAMHAUS(CBL), BRBL, SpamCop, wpbl, UCEPROTECT
  - Malware/Phishing hostsing: SURBL (multi), phishtank, hpHosts
  - Active Attack Behavior: Darknet Scanner (merit), Dshield, ssh brute-force (fail2ban, denyhosts)
- Our goal is to analyze relative distribution of hosts on these lists to determine if there are some common traits that can broadly characterize the observed relative malicious activity originating from a country, ASN, and prefix

LACNIC Address Space Distribution by Country



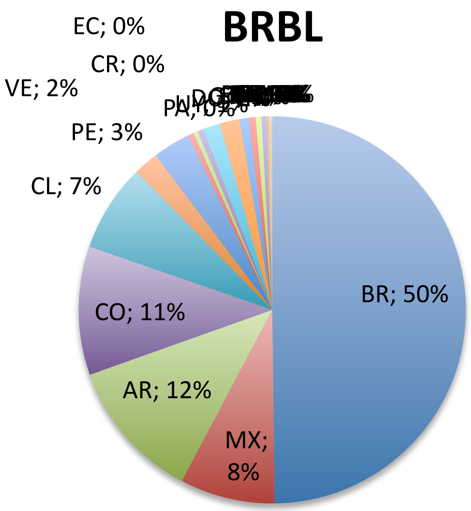
- Roughly 454K/24 blocks allocated ~ 116M IP addresses
- Brazil, Mexico, and Argentina together account for almost 75% of all allocations

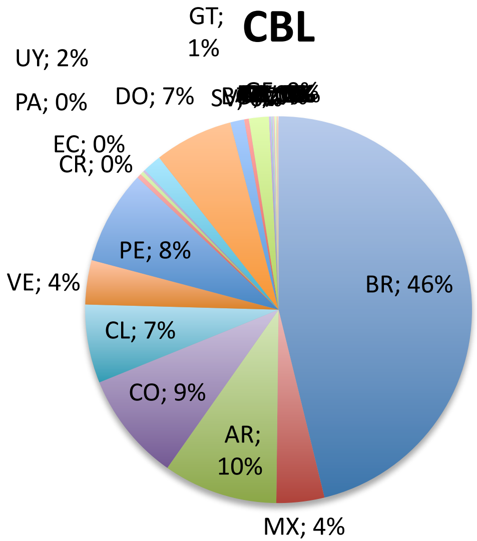


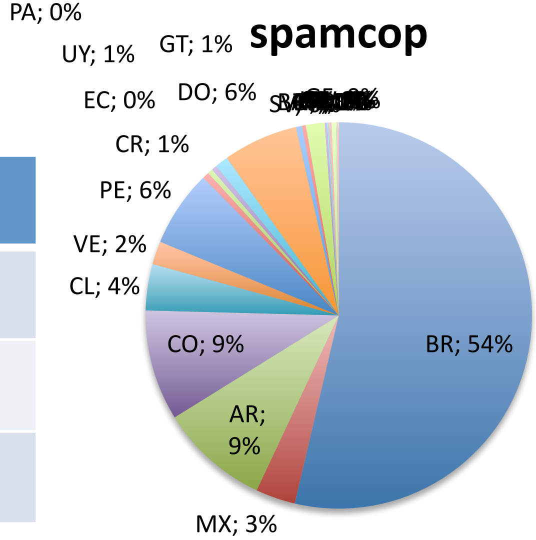
SPAM Lists Distribution Analysis

- Consider 3 largest/most popular SPAM Lists:
  - Barracuda BRBL
  - SPAMHAUS – CBL
  - SpamCop
  - Other SPAM data sources as well such as weighted private block list (wpbl), UCEPROTECT also analyzed but omitted here due to similarity
- Determine portions of those lists relevant to the LACNIC region
- Determine relative distribution by country within LACNIC region

SPAM Lists Distribution by Country





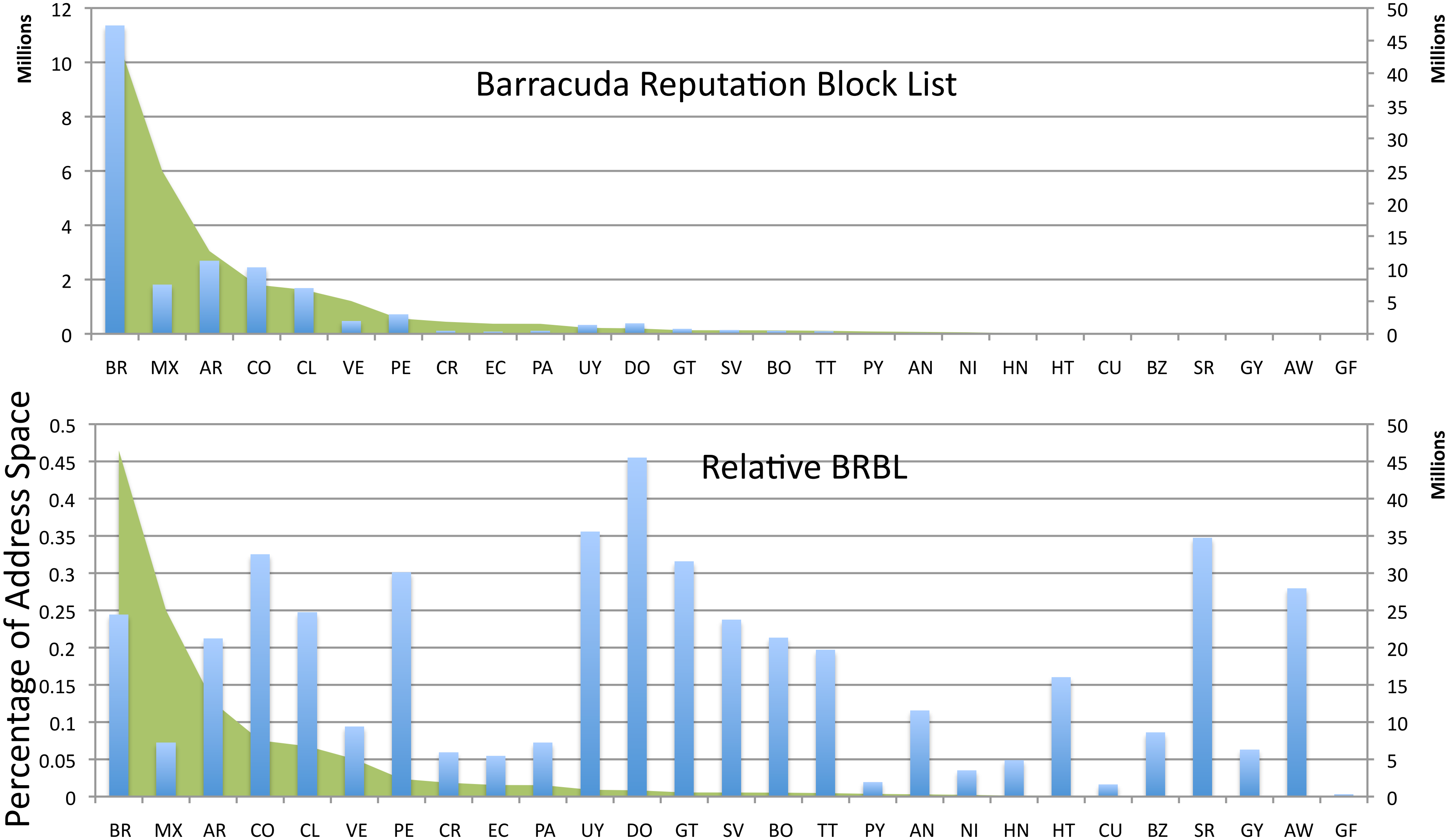


List	Total IPs	LACNIC IPs
Barracuda	128M	22.7M (17%)
SPAMHAUS CBL	8.1M	1M (12%)
SpamCop	325K	28K (8%)

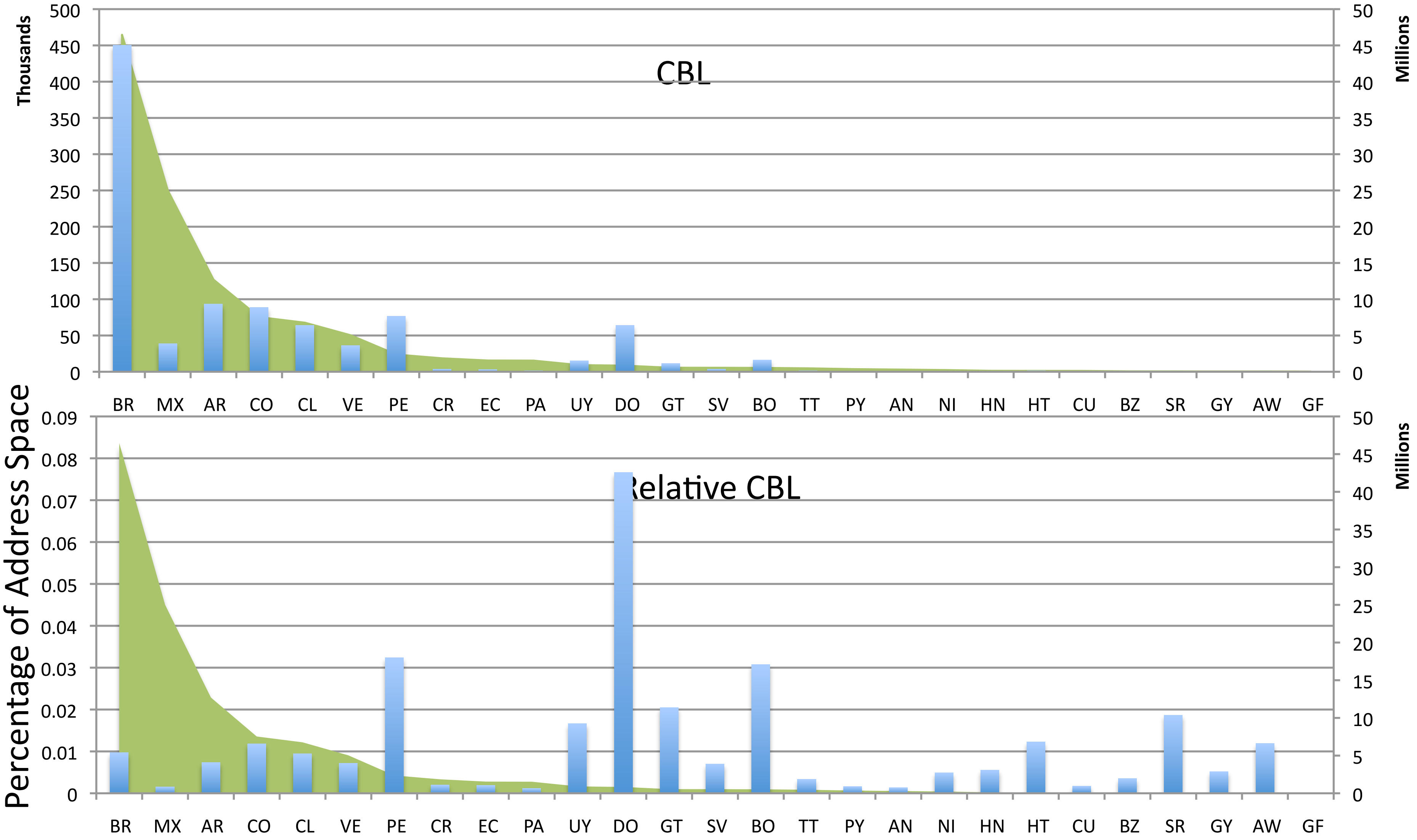
SPAM List Relative Distribution

- In general: countries with larger allocations have more entries in block lists – expected if you assume infection rates are a steady fact of life and on average x% of any given IP address range will be on a block list
- But what happens when we look at block list entries relative to allocation sizes
- We should look at both the large and the small ends of allocation spectrum

Relative SPAM List Distribution by Country



Relative SPAM List Distribution by Country



SPAM List Discussion

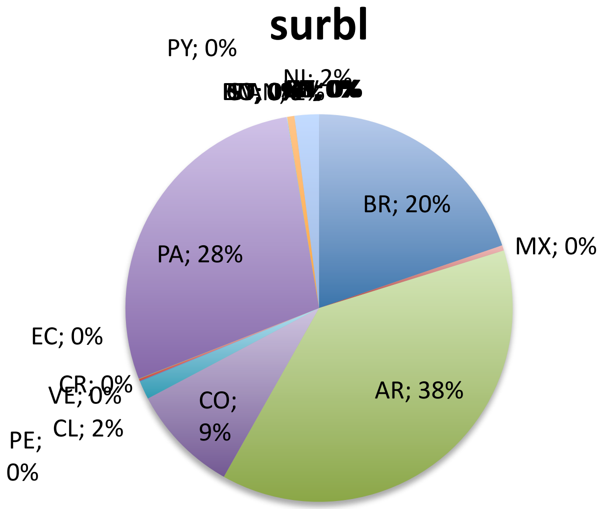
- All networks are not created equal when it comes to entries on a SPAM list
- Interesting things to notice:
  - Almost 45% of Dominican Republic is on BRBL
  - Almost 35% of Uruguay is on BRBL
  - Almost 25% of Brazil is on BRBL but that is 11M IPs
  - More than half of the countries have greater than 10% of their IP addresses on BRBL
  - Only 6% of Mexico IP address space is on BRBL which which is uncharacteristically low
  - CBL stats are lower in terms of absolute numbers but relative trends are consistent

- What accounts for these regional variations? Local policy? Connectivity? Network topology?

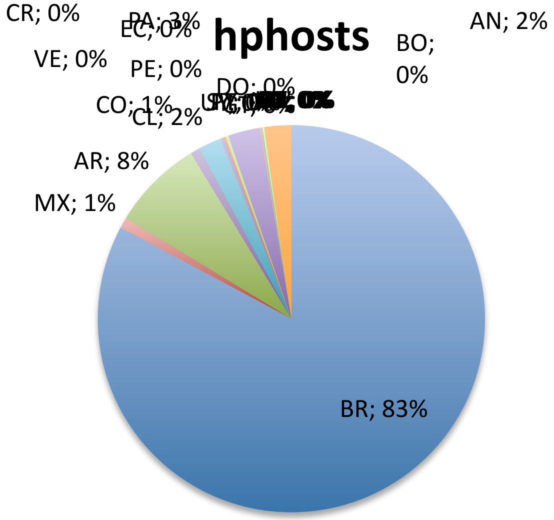
Malware/Phishing Lists Distribution Analysis

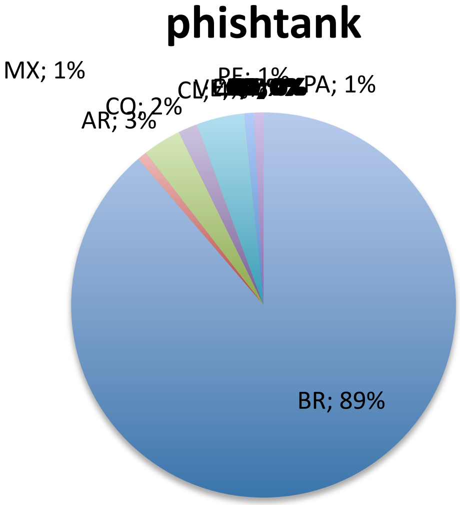
- Consider 3 common malware/phishing Lists:
  - SURBL
  - hpHosts
  - phishtank
  - Other popular data sources as well such as malwaredomains and malwaredomainsList are included in the SURBL-multi dataset.
- Determine portions of those lists relevant to the LACNIC region
- Determine relative country distribution within LACNIC region

Malware/Phishing Lists by Country


surbl

List	Total IPs	LACNIC IPs
SURBL	360K	3K (<1%)
Hphosts	185K	2K (<2%)
Phishtank	4700	124 (< 3%)

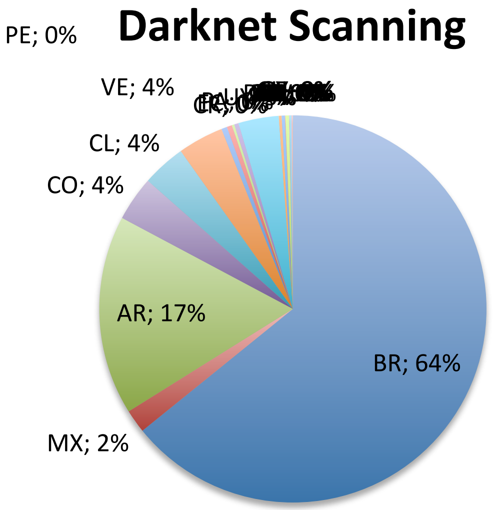

hphosts

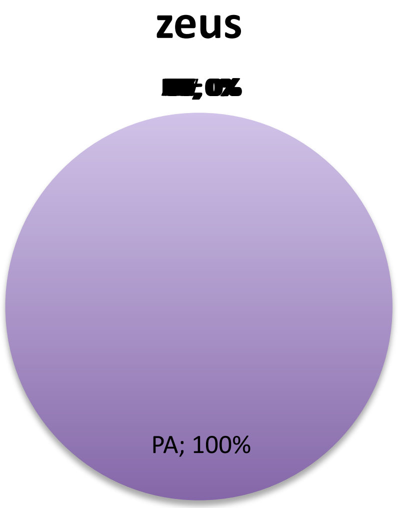

phishtank

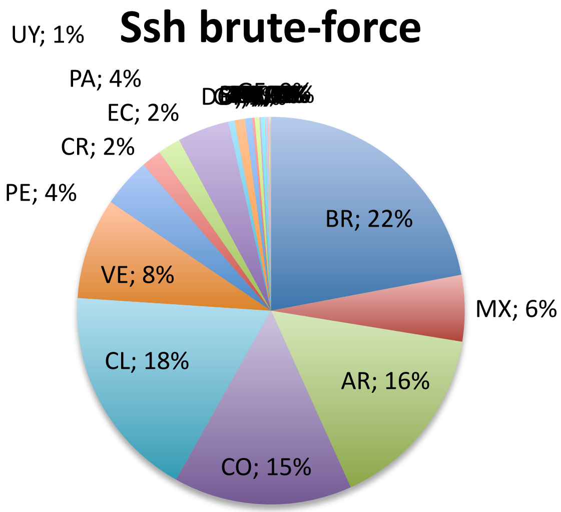
Malware/Phishing Discussion

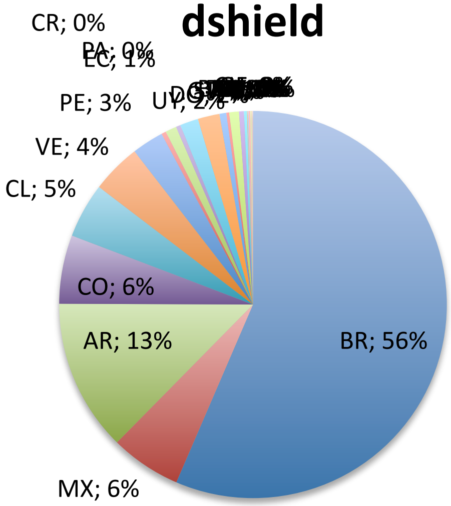
- In general, LACNIC region activity on malware/ phishing lists is uncharacteristically low
- Argentina relatively higher percentage of Malware/Phishing listed domains ~ 40% of all LACNIC region domains on SURBL list.
- Panama and Brazil account for another 30% and 20% of SURBL list respectively. All others much smaller numbers
- Brazil accounts for >80% of entries on hpHosts and phishtank.

Active Malicious Activity by Country







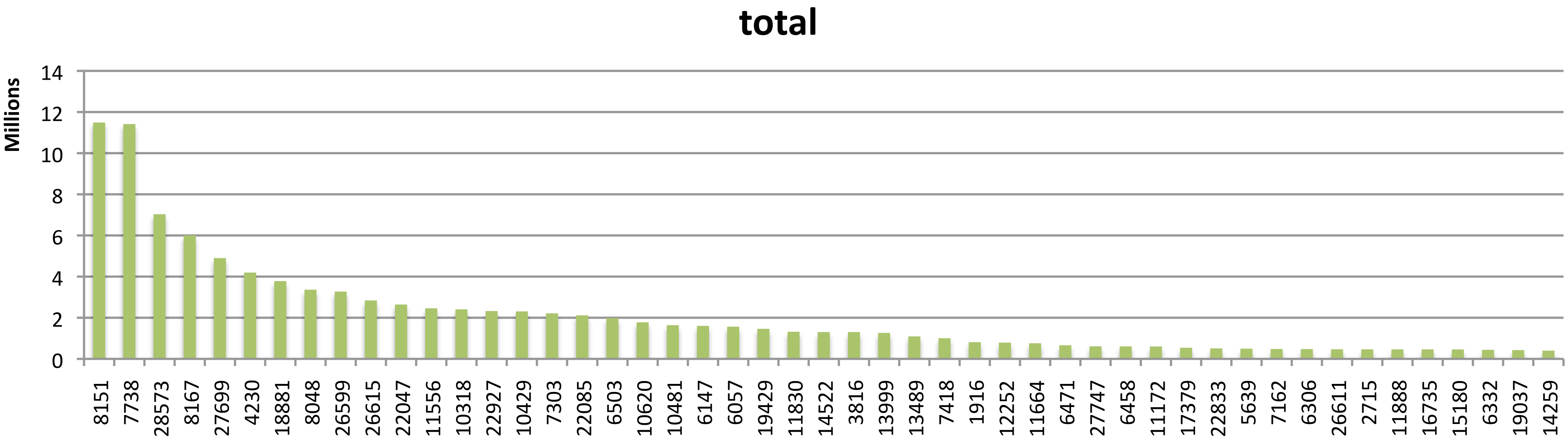


Active Malicious Activity Discussion

List	Total IPs	LACNIC IPs
ssh brute-force	68K	11.6K (17%)
Dshield	754K	61K (8%)
Darknet Scanning	156K	28K (17%)
Zeus	215	1 (0%)

- Brazil is ~ 65% of darknet scanning activity from LACNIC region, Argentina is almost 17% but Mexico is only 2%
- Chile is 18% of ssh brute-force list and Columbia is 15% same as Argentina which is 16% while Brazil is only 22%

Address Distribution by ASN

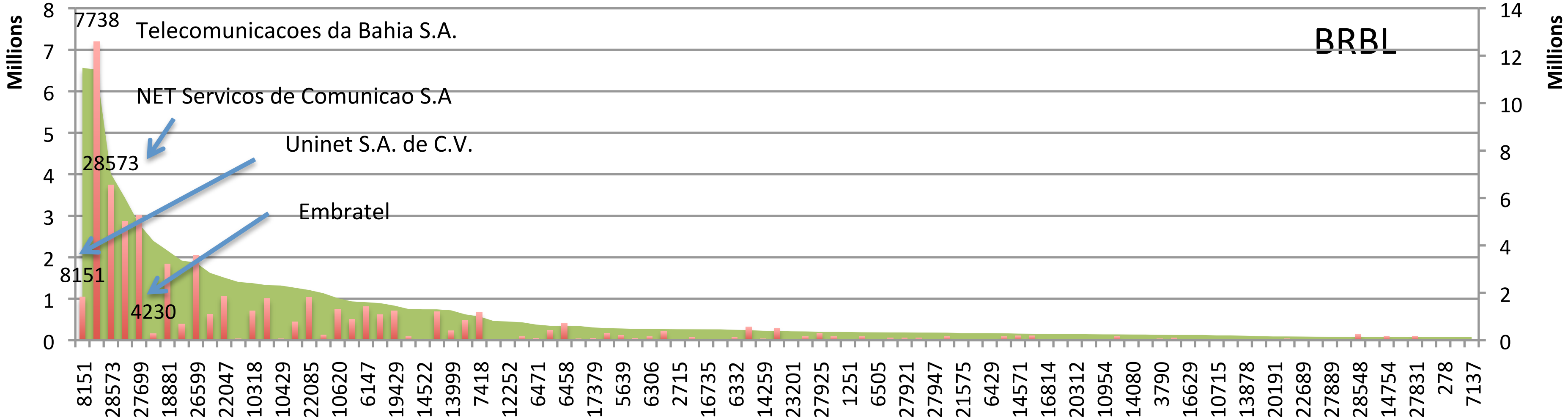


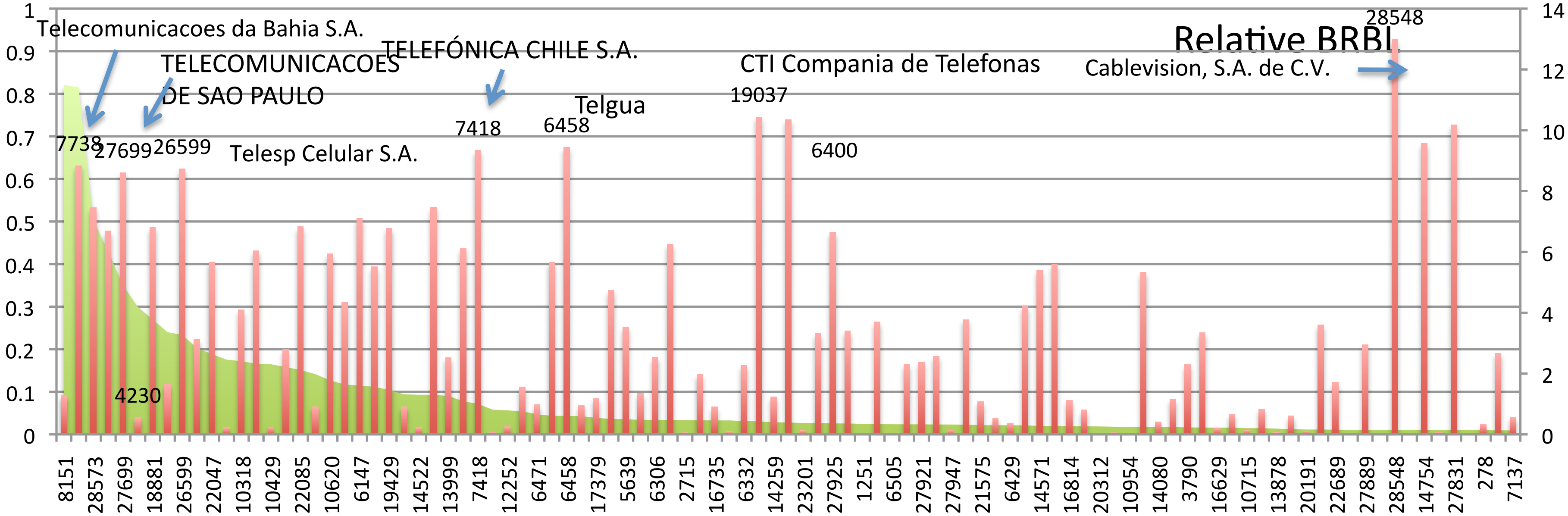
- Roughly 1100 ASNs in use in LACNIC region
- They account for roughly 31K of prefixes in the BGP routing table (total 360K entries)
- A total of 130M IPs
- We focus on the largest 100 ASNs

Top 10 ASNs by Size

ASN	Name	IP Addresses
8151	Uninet S.A. de C.V.	12M (9%)
7738	Telecomunicacoes da Bahia S.A.	12M (9%)
28573	NET Servicos de Comunicao S.A.	7M (5.3%)
8167	TELESC - Telecomunicacoes de Santa Catarina SA	6M (4.6%)
27699	TELECOMUNICACOES DE SAO PAULO S/A - TELESP	4.8M (3.7%)
4230	Embratel	3.7M (2.8%)
18881	Global Village Telecom	3.3M (2.5%)
8048	CANTV Servicios, Venezuela	3.2M (2.4%)
26599	Telesp Celular S.A.	2.8M (2.1%)
26615	Tim Celular S.A.	2.6M (2%)

SPAM List IP Distribution by ASN

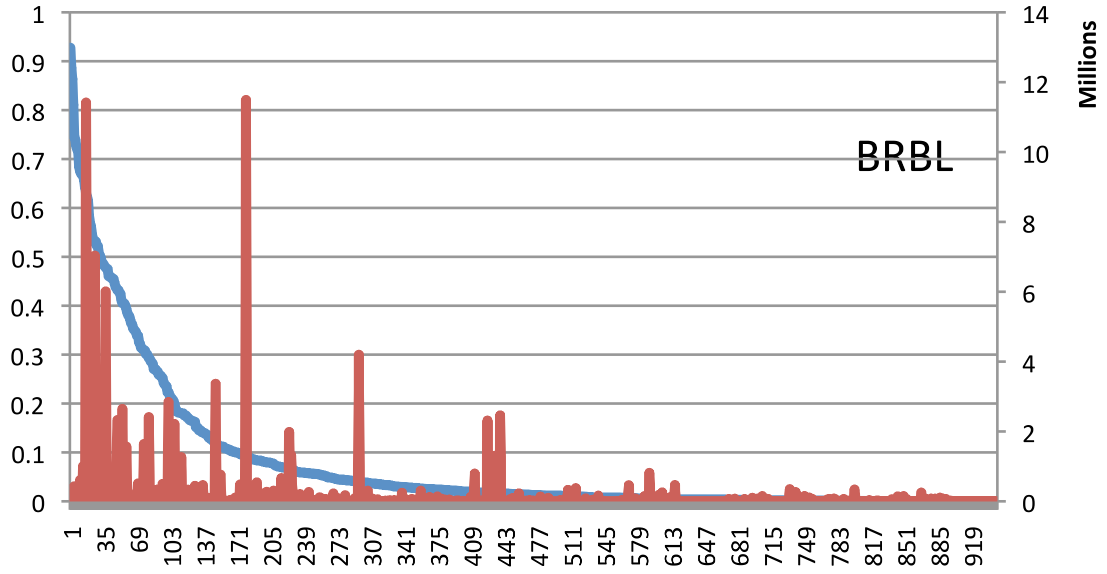


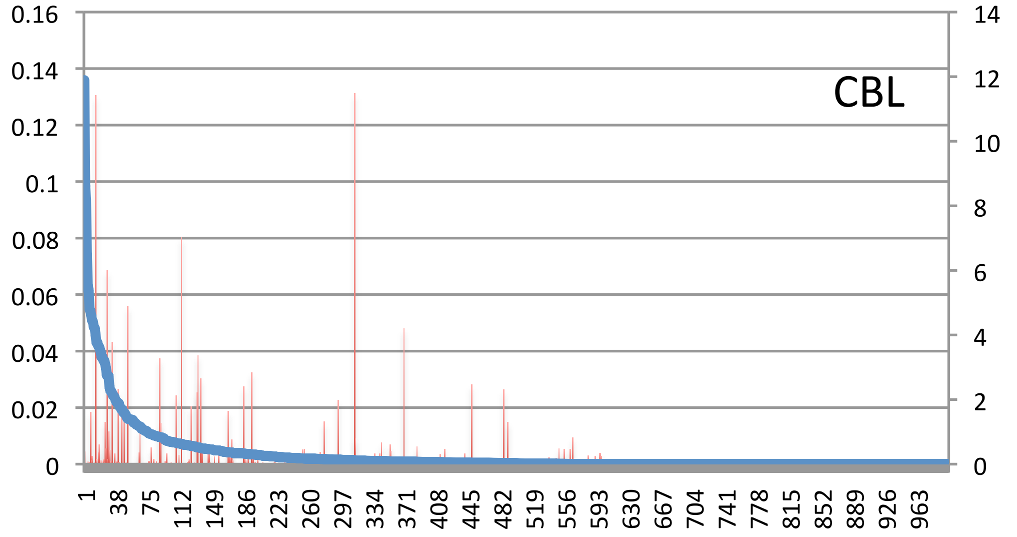


SPAM List IP Address Distribution by ASN Discussion

- Top 10 network AS7738 - Telecomunicacoes da Bahia S.A. accounts for over 7M IPs on BRBL which is over 60% of its total address space
- AS 8151- Uninet S.A. de C.V and AS7738 - Telecomunicacoes da Bahia S.A. both have almost same amount of amount of address space 11M IPs yet AS 8151 has only 1M addresses on BRBL
- AS28548 - Cablevision, S.A. de C.V. is almost entirely on BRBL
- 18 of the largest 100 ASNs have more than 50% of their address space on the BRBL
- AS4230 – Embratel has over 3M IPs but relatively negligible number of entries on BRBL

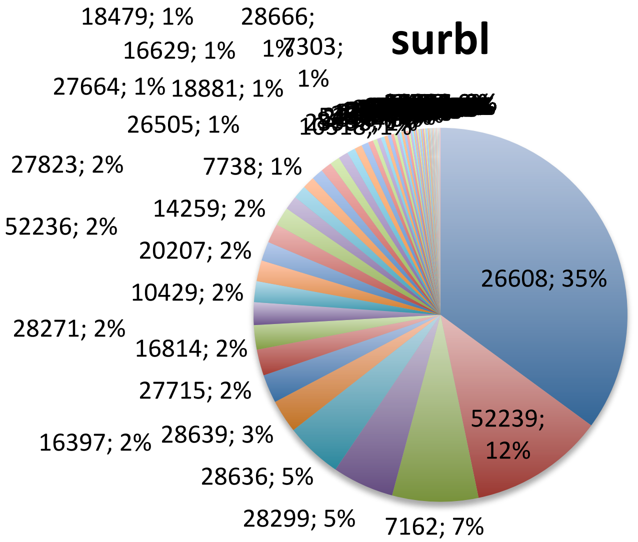
ASN IP Blocklisting Distribution

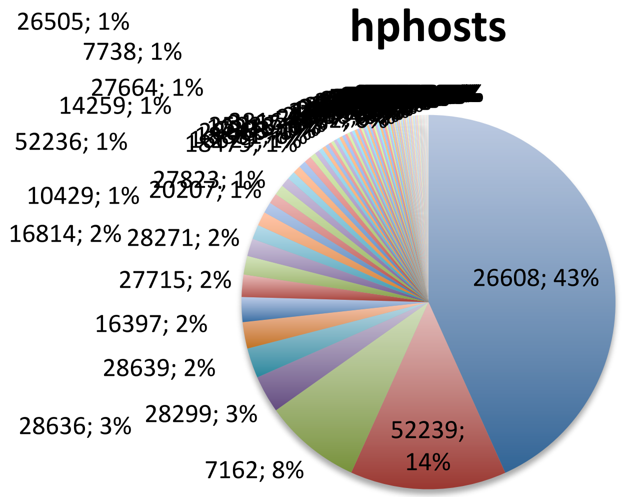


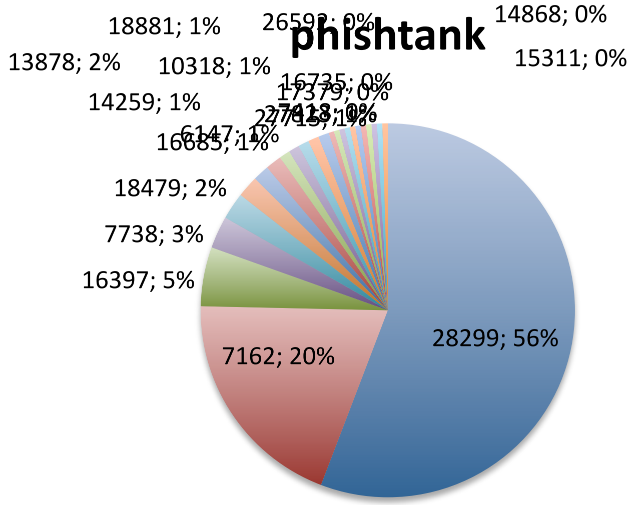


- Top 1000 ASNs with largest percentage of their networks on SPAM blocklists
- Almost 100 ASNs have atleast 20% of their IPs on BRBL
- Almost 40 ASNs have atleast 2% of their IPs on CBL

Malware/Phishing Domains Distribution by ASN

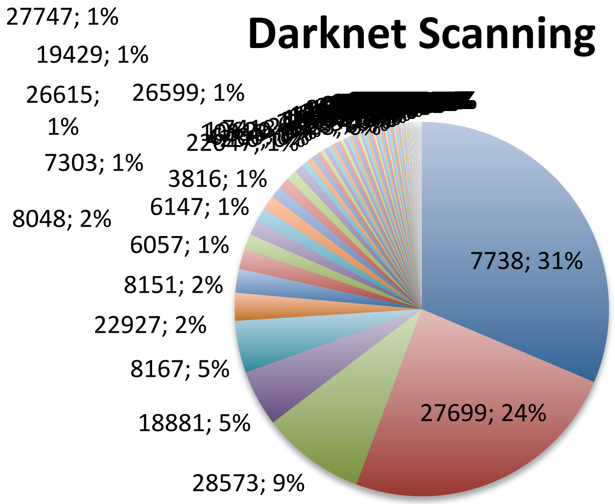


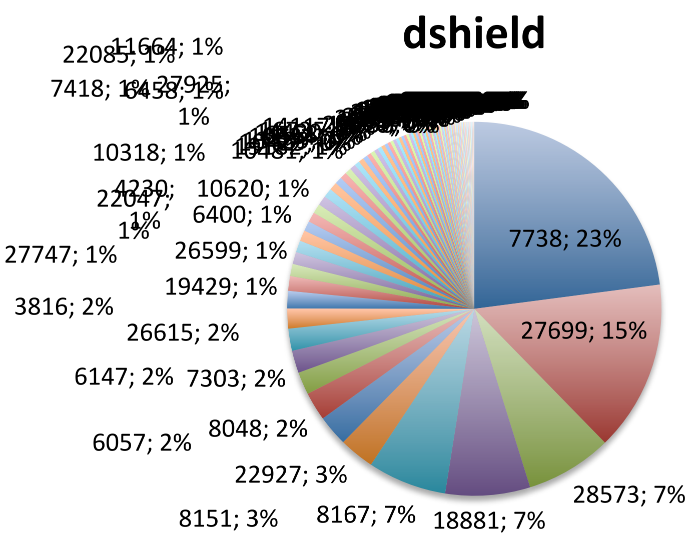


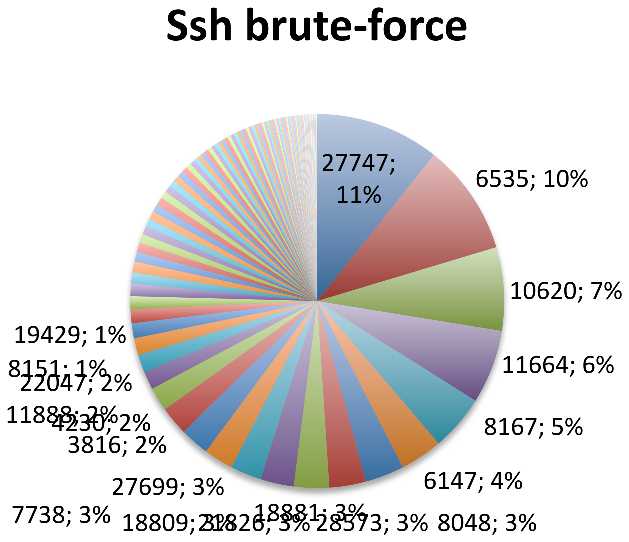


- AS26608 - SkyOnline de Argentina, represents 35% of SURBL LACNIC region entries and 43% of hphosts entries
- AS 52239 - Desarrollos Digitales is the next highest contributor with 12% and 14%
- AS 282997 - CYBERWEB is almost 56% of LACNIC region phishtank entries. and AS7162 Itanet – is 20% of phishtank entries
- Consistency across surbl and hpHosts entries but different ASN with phishtank

Active Malicious Activity by ASN







AS 7738 - Telecomunicacoes da Bahia S.A.

AS 27699 - TELECOMUNICACOES DE SAO PAULO

AS 27747 - Telecentro S.A.

AS 28573 - NET Servicos de Comunicao S.A.

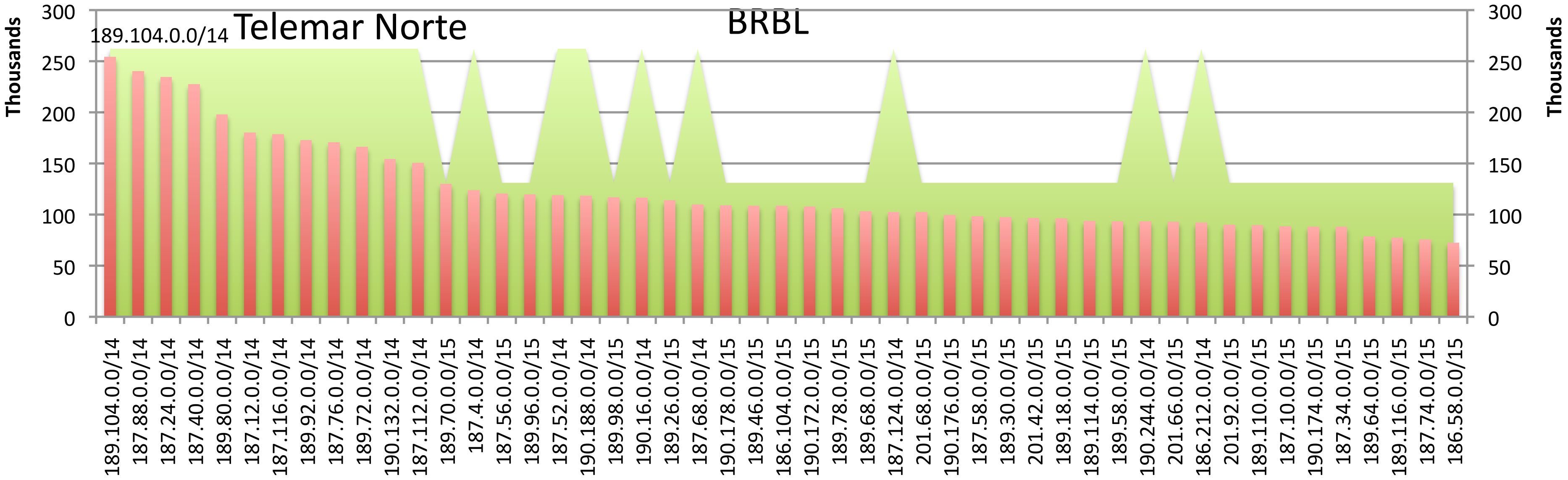
AS6535 - Telmex Servicios

Active Malicious Activity Discussion

List	Total IPs	LACNIC IPs
ssh brute-force	68K	11.6K (17%)
Dshield	754K	61K (8%)
Darknet Scanning	156K	28K (17%)
Zeus	215	1 (0%)

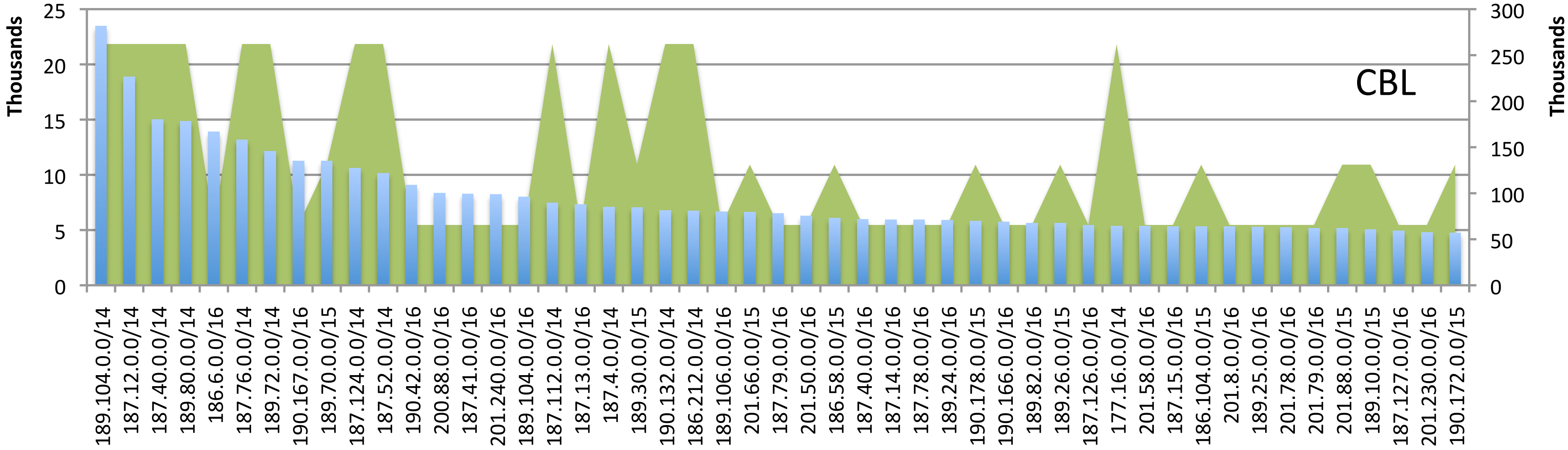
- AS7738 - Telecomunicacoes da Bahia represents 31% of all darknet scanning activity from LACNIC region and AS 27699 represents another 24%
- Consistency between Darknet scanners list and Dshield data
- AS 6535 - Telmex Servicios, Mexico accounts for 10% of ssh brute-force entries

BGP Prefix SPAM List IP Distribution



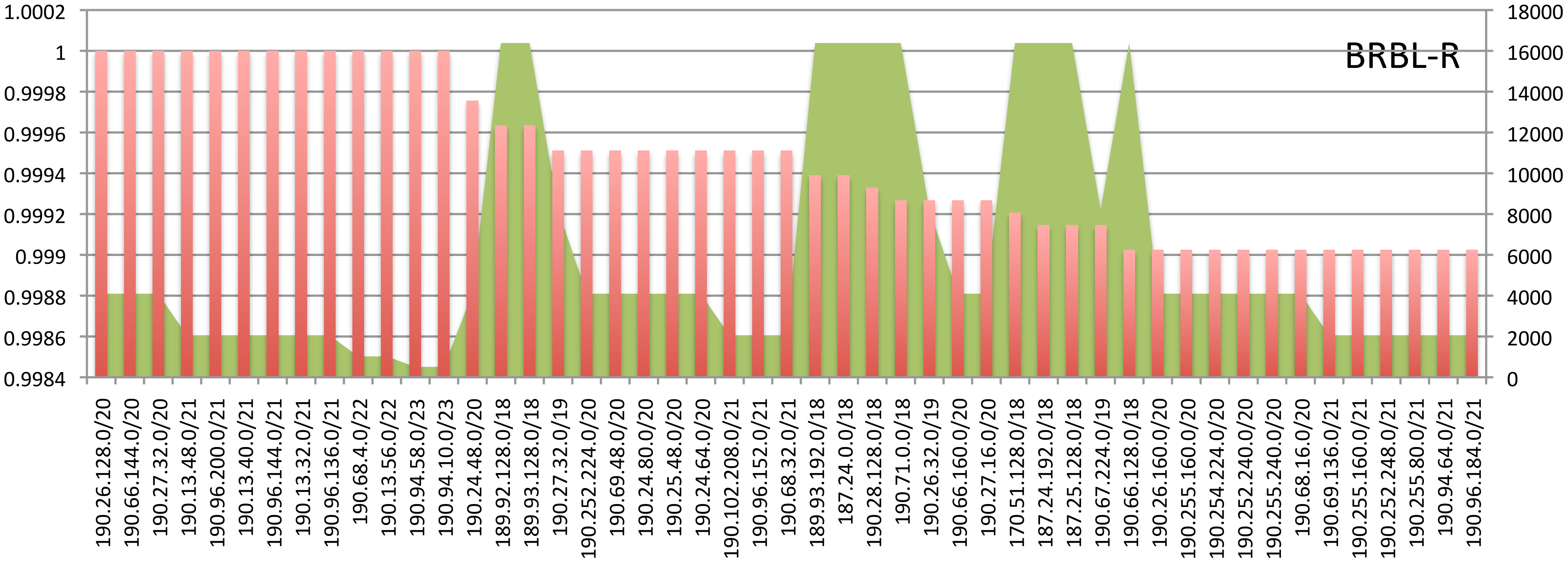
- BGP LACNIC region prefixes 31290 out of total routing table of ~370K
- No surprise that large prefixes have large numbers of IPs in BRBL
- BUT – still a surprise that 12 prefixes (all /14s) have over 150K IPs in the BRBL
- 189.104.0.0/14– Telemar Norte has 250K IPs out of an allocation of 254K on BRBL
- 187.88.0.0/14- Vivo S.A has 240K IPs out of254K on BRBL
- All 50 prefixes shown above have atleast 50K IPs on BRBL the equivalent of 195 /24 blocks

BGP Prefix SPAM List IP Distribution



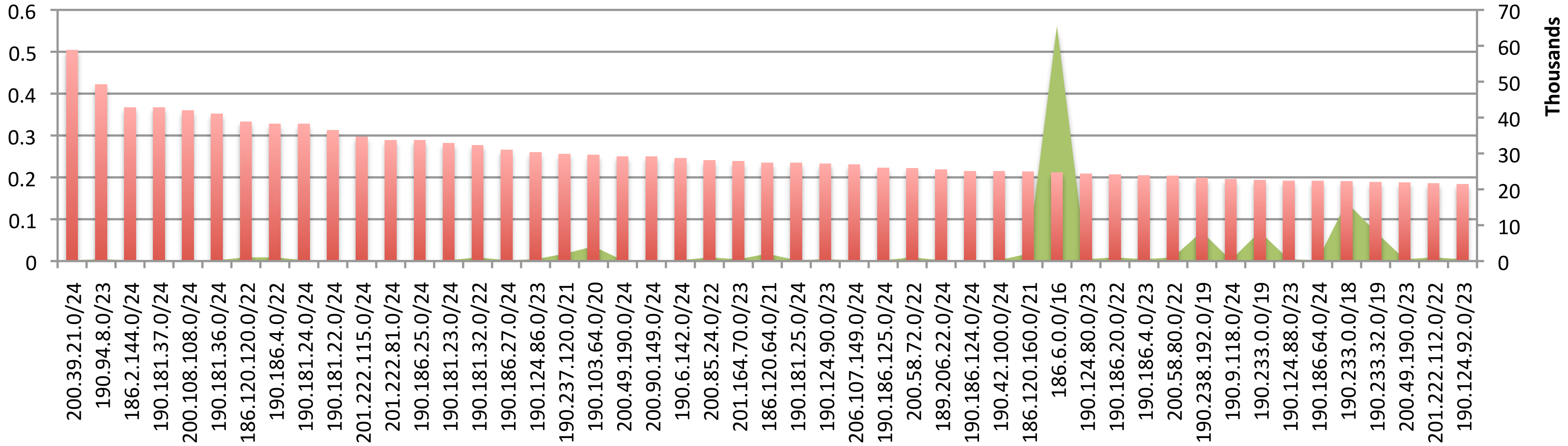
- Even for CBL all 50 of the prefixes shown above have almost 5K or more IPs listed
- 189.104.0.0/14 – Telemar Norte has almost 23K IPs listed in the CBL
- 187.12.0.0/14 - Comite Gestor da Internet no Brasil - has roughly 18K IPs listed in CBL

Relative Amounts of IP addresses in SPAM lists



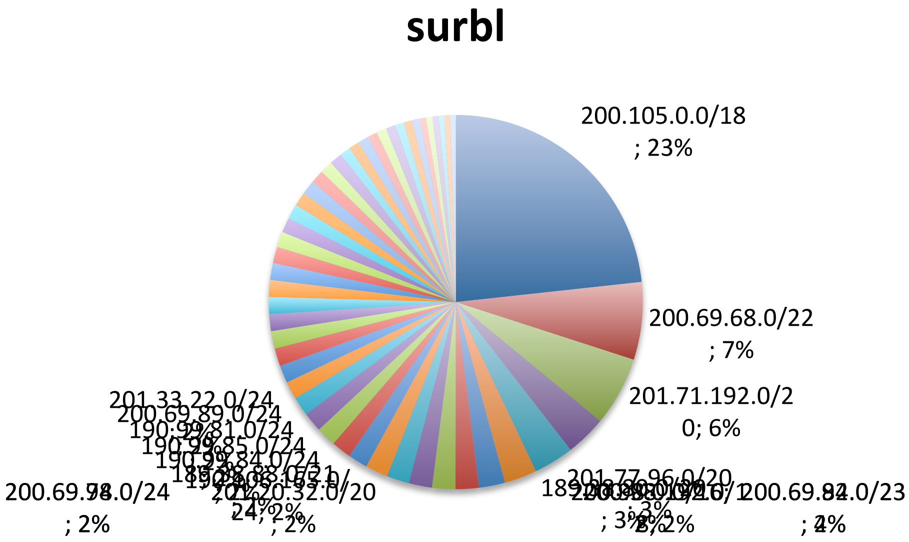
- 2000 LACNIC region prefixes have over 90% of their address space included in the BRBL
- Over 5300 prefixes out of all LACNIC region prefixes have more than 50% of their IP address block listed in the BRBL

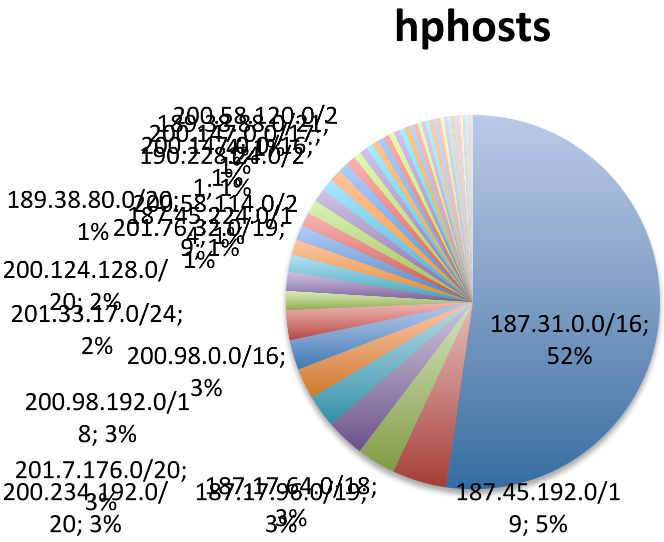
Relative Amounts of IP Address in SPAM Lists



- 40 prefixes have atleast 20% of their IPs listed in CBL
- 200.39.21.0/24 - Pegaso PCS, Mexico has 50% of its space on CBL but 186.6.0.0/16 – CODETEL has 55% of its block on CBL

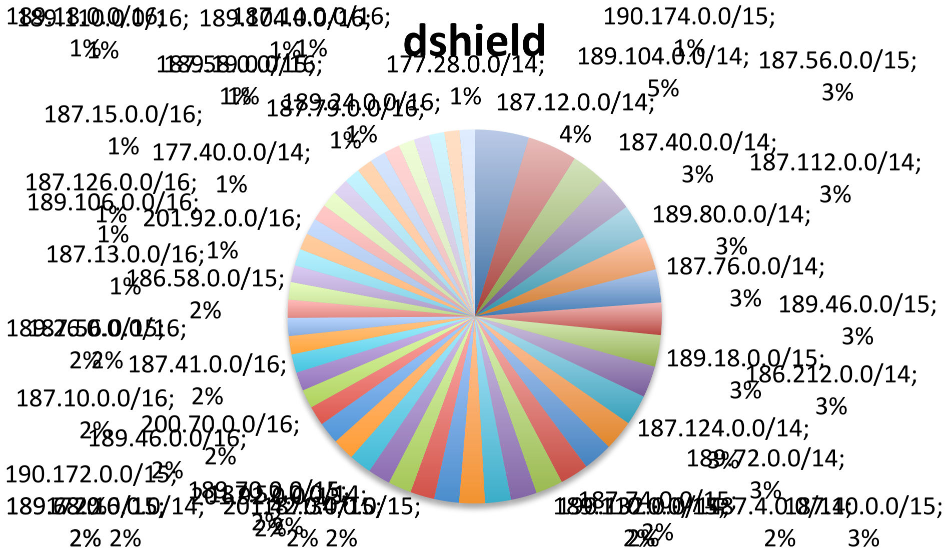
Malware/Phishing IP Address Distribution

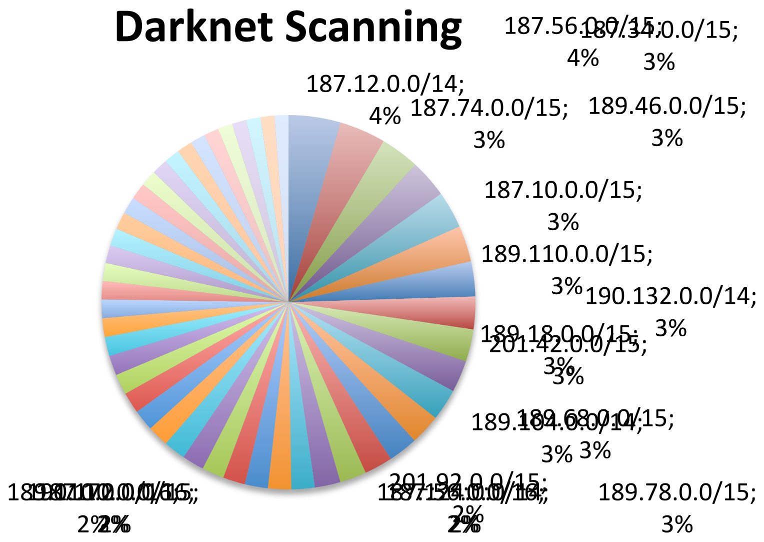


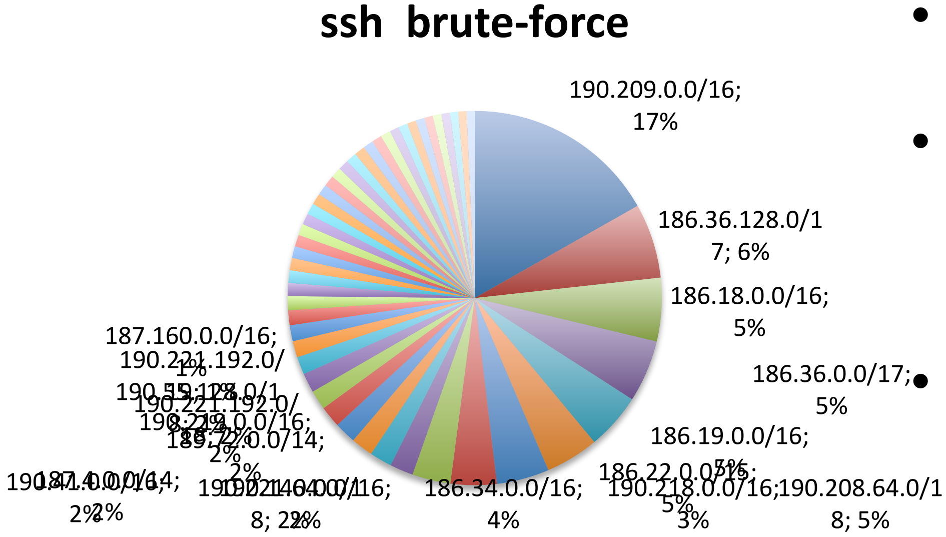


- Relative percentages of IPs for the top 50 prefixes for each data type are shown above
- 200.105.0.0/18 – SkyOnline, Argentina represents 23% of all surbl entries from top 50 prefixes
- 187.31.0.0/16 - Internet Group, Brazil represents 50% of hpHosts entries.

Active Malicious Activity List IP Distribution







- Relative percentages of IPs in the top 50 prefixes are shown above
- No clear outliers in terms of prefixes which have exceptional Darknet scanning activity or Dshield entries
- 190.209.0.0/16, 186.36.128.0/17 – TELMEXCHILE represents 25% of ssh brute-force attempts

Discussion

- Network reputation is an attempt to construct a metric or set of metrics that illustrate the collective reputation of all hosts in your administrative domain
- While infected hosts and botnets are a fact of life, how much of such activity represents an acceptable level of network pollution 1%? 10% of all hosts?
- Hosts that engage in malicious activity such as spam, phishing, malware, scanning in a network reduce the externally visible global network reputation of that network – it does not go un-noticed
- It can be seen that not all networks are equal when it comes to network reputation. What policies, topology, connectivity, other factors make some networks better than others? How can we learn from them?
- Reputation of hosts on your network has an impact on the usability of your network as portions might get blocked for various services

Using Network Reputation

- Network reputation is not just something other people know about you
- You can use it to craft flexible local policies that can better manage your risk profile
- Variable services can be offered to networks with different reputations
- You can control how much of your network and what services on your network are visible to networks with varying reputation levels
- Reputation information can even be a factor in BGP path selection algorithm

Network Reputation

- Our goal is to develop a comprehensive global network reputation system that computes for each prefix in the BGP routing table a reputation metric.
- Variations can allow arbitrary network boundaries not simply BGP boundaries but that is the starting point
- Data from common sources such as RBLs is the starting point for bootstrapping the reputation system, however in order to be successful the system must have data from many many vantage points
- Different networks have different views of reputations of other networks
- The more vantage points you have the closer to "true reputation you will get"
- The system must allow all networks to participate and contribute reputation information regarding all other networks while being resistant to collusion and false reporting
- Current project at Merit Network Inc is building such a system and an effort will soon be made to recruit participant networks on various mailing lists
- If you would like to participate please send email to: mkarir@merit.edu
- How reputable is your network?